UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------x
UNITED STATES OF AMERICA,

-against-

NARAY PALANIAPPAN,

Defendant.
----------x

MEMORANDUM AND ORDER
15-CR-485 (FB)

BLOCK, Senior District Judge:

The defendant is charged with receipt and possession of child pornography. This memorandum and order addresses his (1) motion to suppress evidence, (2) motion to dismiss the indictment, and (3) motion to compel discovery. For the following reasons, the motions are denied.

1. Motion to Suppress

The Court holds that use of the Network Investigative Technique ("NIT") was a search and that the warrant for the search violated the geographic limitation of Federal Rule of Criminal Procedure 41(b)(1) in effect at the time.[1] The Court need not decide whether the violation was of constitutional magnitude, however, because suppression is not an appropriate remedy in either case.

---

[1]The Rule has since been amended—specifically to address concerns about the NIT warrant—to allow magistrates in any district to issue warrants "to use remote access to search electronic storage media . . . located within or outside that district." Fed. R. Crim. P. 41(b)(6).

"[V]iolations of Rule 41 alone should not lead to exclusion unless (1) there was prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule." *United States v. Burke*, 517 F.2d 377, 386-87 (2d Cir. 1975). There was no prejudice because the FBI could have obtained the same warrant from a district judge, *see United States v. Villegas*, 899 F.2d 1324, 1334 (2d Cir. 1990) ("[Rule 41] does not define the extent of the [district] court's power to issue a search warrant."), and because the FBI complied with the extended deadline for giving the defendant notice of the warrant.

Nor did the FBI intentionally and deliberately disregard Rule 41's geographical limitation on the magistrate judge's authority. The Playpen website's efforts to protect its users' anonymity posed a novel problem. The FBI disclosed the salient facts about its proposed solution to the magistrate judge, including the fact that the NIT would be installed on a server in Virginia, but deployed on any computer accessing the server, regardless of location. This reflects a reasoned judgment as to how to comply with Rule 41 in unique circumstances, not an attempt to flout it.

Even if the violation of Rule 41 was of constitutional magnitude, the good-faith exception of *United States v. Leon*, 468 U.S. 897 (1984), forecloses suppression. The unique circumstances made it reasonable for the FBI to rely on the magistrate judge's determination that she could authorize a remote search from a computer located in the

Eastern District of Virginia. *See id.* at 920 ("In the ordinary case, an officer cannot be expected to question the magistrate's probable-cause determination or his judgment that the form of the warrant is technically sufficient."). Contrary to the defendant's contention, the warrant did not, on its face, limit use of the NIT to computers located in the district. The problems that might create under Rule 41 were not so obvious as to make the executing officers' reliance on the warrant unreasonable. *See United States v. Workman*, 863 F.3d 1313, 1321 (10th Cir. 2017) ("We expect agents executing warrants to be reasonably well-trained, but we do not expect them to understand legal nuances the way that an attorney would.").

2. Motion to Dismiss

"Government involvement in a crime may *in theory* become so excessive that it violates due process and requires the dismissal of charges against a defendant even if the defendant was not entrapped." *United States v. Al Kassar*, 660 F.3d 108, 121 (2d Cir. 2011) (emphasis added). But "only Government conduct that 'shocks the conscience' can violate due process." *United States v. Rahman*, 189 F.3d 88, 131 (2d Cir. 1999). The burden of showing sufficiently outrageous conduct is "very heavy," *id.*, principally because courts are reluctant to abandon their "well-established deference to the Government's choice of investigatory methods." *Id.* "It does not suffice to show that the government created the opportunity for the offense, even if the government's ploy is elaborate and the engagement with the defendant is

extensive." *Al Kassar*, 660 F.3d at 121.

Generally, "the government's involvement in a crime must involve either coercion or a violation of the defendant's person," *id.*, neither of which is present here. In *United States v. Chin*, 934 F.2d 393 (2d Cir. 1991), however, the Second Circuit concluded that a lack of harm to the defendant "does not end our analysis," *id.* at 399, and went on to consider the harm to third parties and, in particular, the victims of child pornography:

> Our concern is that, in contrast to the usual sting operation, in which the Government sets up a phony drug transaction or another sort of dummy crime, the government agent in this case encouraged Chin to go out and commit a real crime, with real victims, just so Chin could later be arrested and prosecuted. In particular, [an undercover postal inspector] explicitly and repeatedly encouraged Chin to proceed with his trip to Amsterdam to obtain "Lolita materials," despite the fact that purchasing child pornography, by increasing the demand for such materials, serves to further the sexual exploitation of minors.

Id. The circuit court "cautioned law enforcement agents to think twice before engaging in investigative techniques that encourage individuals to commit actions that harm innocent third parties," *id.* at 400, but did not dismiss the indictment because the defendant could not establish "[a] necessary prerequisite for demonstrating that an undercover investigation violated the rights of third parties," *id.*, namely, "proof that the governmental action actually caused the defendant to commit a crime that would otherwise not have been committed," *id.*

Here, the FBI delayed shutting down an existing website for two weeks. The

child pornography itself was uploaded and retrieved by users like the defendant, just as it had been before February 20, 2015. Moving the site to a government server obviously meant greater government involvement, but the harm to victims was the same as letting the website continue to operate from its original server. The decision to leave the site operational arguably "created the opportunity for the offense," *Al Kassar*, 660 F.3d at 121, but it did not encourage the defendant or anyone else to visit the site.

Of course, the FBI could have decided to shut down the site immediately and prevent the further distribution of the images it hosted. But that option would have meant leaving users of the site unidentified and unapprehended, free to continue sharing child pornography by other means. *See United States v. Kim*, 2017 WL 394498, at *7 (E.D.N.Y. Jan. 27, 2017) ("[T]here is no evidence upon which the Court can conclude that individuals interested in child pornography would have been so easily deterred from obtaining it by the shutting down of the Playpen website."). Whether an immediate shutdown or a delay would have best served the long-term effort to combat child pornography is precisely the kind of difficult decision that courts should not second-guess.

3. Motion to Compel

Federal Rule of Criminal Procedure 16(a)(1)(E)(i) (E) requires the government to produce any item within its custody or control that is "material to preparing the

defense." The defendant argues that the "exploit code" that allowed the NIT to take advantage of a software vulnerability on the defendant's computer is material in two ways.

First, he argues that the exploit code might allow him to investigate whether the NIT transmitted information from his computer beyond the scope of the warrant authorizing its use. Rule 16 deals with information material to the defendant's case on the merits, not collateral issues like a motion to suppress. *Cf. United States v. Armstrong*, 517 U.S. 456, 463 (1996) ("Rule 16(a)(1)(C) authorizes defendants to examine Government documents material to the preparation of *their defense against the Government's case in chief*, but not to the preparation of selective-prosecution claims." (Emphasis added)).

Second, he argues that the exploit code might reveal that the NIT left his computer vulnerable to hacking, thus bolstering a claim that the pornography found on his computer was placed there without his knowledge. This would be speculative under the best of circumstances, but the defendant has already admitted to agents that he visited the website and downloaded the images he is charged with possessing.

SO ORDERED.

/S/ Frederic Block___
FREDERIC BLOCK
Senior United States District Judge

Brooklyn, New York
April 27, 2018